An Overview and Analysis of Private and Public Key DNA Cryptography

K.Sireesha
Assistant Professor
Department of Computer Science & Engineering
K L University, Green Fields, Vaddeswaram
Guntur District, Andhra Pradesh

V.Srujana
Assistant Professor
Department of Computer Science & Engineering
K L University, Green Fields, Vaddeswaram
Guntur District, Andhra Pradesh

***Abstract*—with the growth of technological advancements, the threats dealt by a user grow exponentially. Hence security has become a critical issue in data storage and transmission. As traditional cryptographic systems are now vulnerable to attacks, the concept of using DNA Cryptography has been identified as a possible technology that brings forward a new hope for unbreakable algorithms. This paper analyzes the different approaches on DNA based Cryptography**

Keywords: ***Cryptography; SK;, AK;, PKC; DES; DNA based Cryptography.***

I. INTRODUCTION

Sensitive information such as financial transactions, medical and personal records are transmitted through public communication facilities. The security of the sensitive information poses a great threat by an unintended recipient. Cryptographic techniques help in ensuring the security of such sensitive information. Cryptography enables the sender to securely store or transmit sensitive information across insecure networks so that it can be understood only by the intended recipient. A cryptographic system applies encryption on the information and produces an encrypted output which will be meaningless to an unintended user who has no knowledge of the key. Knowledge of the key is essential for decryption. The fundamental tool for cryptography is the one way function. A function is one-way if it is easy to compute but hard to invert. A one-way function is a function f, such that for each x in the domain of f, it is easy to compute f(x); for essentially all y in the range of f, it is computationally infeasible to find any x, such that y = f(x). A trapdoor one-way function is a one-way function, f with the additional property that given some extra information (the trapdoor information), it becomes computationally feasible to compute for any y in the range of f an x, such that y = f(x).

Cryptography can be broadly classified as Symmetric Key Cryptography (SKC) and Asymmetric Key Cryptography (AKC). Symmetric Key Cryptography uses the same key for both encryption and decryption as shown in Fig 1. Asymmetric Key Cryptography also known as Public Key Cryptography (PKC) uses separate keys for encryption and decryption as shown in Fig 2.

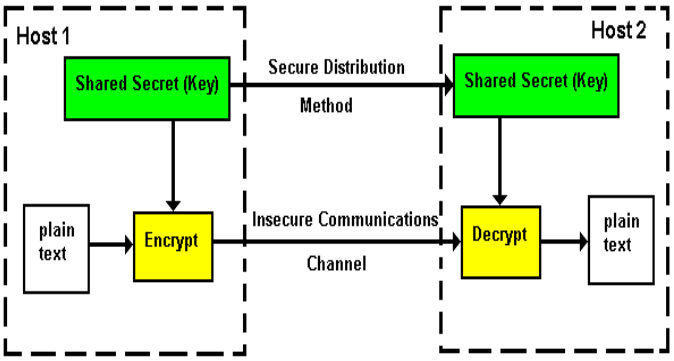

Figure 1. Symmetric Key Cryptography

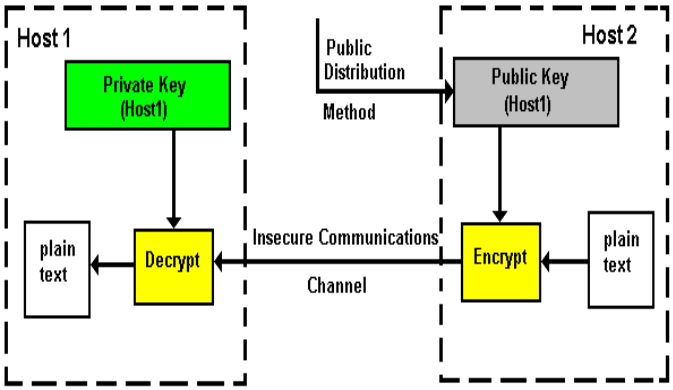

Figure 2. Asymmetric Key Cryptography

An important characteristic of PKC algorithms is that it should be computationally infeasible to determine the decryption key given only the knowledge of the algorithm and the encryption. The security of the encrypted information is entirely dependent on the strength of the cryptographic algorithm and the keys used for encryption and decryption. In secure encryption schemes, the legitimate user is able to decipher the messages (using some private information available), yet for an adversary (not having this private

information) the task of decrypting the cipher text (i.e., "breaking" the encryption) should be infeasible. But today, the breaking task can be performed by a non-deterministic polynomial-time machine.

The Data Encryption Standard (DES) is an algorithm with approximately 72 quadrillion possible keys. The security of the DES is based on the difficulty of picking out the right key after the 16-round nonlinear function operations. Breaking DES by molecular computer proposed by Boneh and the Molecular Sticker algorithm proposed by Zhihua Chen indicate that molecular computing has the ability to break DES [15] [16]. Though cryptography enables in ensuring security to sensitive information, code breakers have come up with various methods to crack the cryptographic system [4]. As traditional cryptographic methods built upon mathematical and theoretical models are vulnerable to attacks, the concept of using DNA computing in the field of cryptography has been identified as a possible technology that brings forward a new hope for unbreakable algorithms.

II. DNA COMPUTING

DNA stands for Deoxyribo Nucleic Acid. DNA represents the genetic blueprint of living creatures. DNA contains "instructions" for assembling cells. Every cell in human body has a complete set of DNA. DNA is unique for each individual. DNA is a polymer made of monomers called deoxyribo nucleotides. Each nucleotide consists of three basic items: deoxyribose sugar, phosphate group and a nitrogenous base. The nitrogenous bases are of two types: purins (Adenine and Guanine) and pyrimidins (Cytosine and Thymine). They are represented as A, G, C and T. A binds with T and G binds to C. The various operations that can be performed on DNA are ligation, polymerase chain reaction (PCR), gel electrophoresis and affinity purification.

DNA computing is an inter-disciplinary area concerned with the use of DNA molecules for the implementation of computational processes. The main features of DNA are massive parallelism and complementarity as proposed by Watson and Crick [15]. Adleman's pioneering work gave an idea of solving the directed Hamiltonian Path Problem (Travelling Salesman Problem) of size n in O(n) using DNA molecules [1]. The principle used by Adleman lies in the coding of information (nodes, edges) in DNA clusters and in the use of enzymes for the simulation of simple calculations. Lipton extended the work of Adleman and investigated the solution of Satisfiability of Propositional Formula pointing to new opportunities of DNA computing [8].

III. DNA BASED CRYPTOGRAPHY

Research work is being done on DNA Computing either using test tubes (biologically) or simulating the operations of DNA using computers (Pseudo or Virtual DNA computing). Gehani et. al., introduced the first trial of DNA based Cryptography in which a substitution method using libraries of distinct one time pads, each of which defines a specific, randomly generated, pair-wise mapping and an XOR scheme utilizing molecular computation and indexed, random key strings are used for encryption [2]. An image encryption algorithm based on DNA sequence addition operation is presented by Wang et. al. [10]. A DNA sequence matrix is obtained by encoding the original image and it is divided into some equal blocks and two logistic maps, DNA complementarity and DNA sequence addition operation are utilized to add these blocks. DNA sequence matrix is decoded to get the encrypted image.

Leier et. al. presented two different cryptographic approaches based on DNA binary strands with the idea that a potential interceptor cannot distinguish between dummies and message strand [7]. The first approach hid information in DNA binary strands and the second designed a molecular checksum. Decryption is done using PCR and subsequent gel electrophoresis. The YAEADNA algorithm proposed by Sherif et. al. uses a search technique in order to locate and return the position of quadruple DNA nucleotide sequence representing the binary octets of plain text characters [12]. Plain text character and a random binary file are given as input and the output PTR is a pointer to the location of the found quadruple DNA nucleotide sequence representing the binary octet. The encryption process was tested on images to show how random the selection of DNA octet's locations is on the encrypting sequence. Kang explained the pseudo encryption methodology based upon the work of Ashish Gehani et. al. [9].

The plain text is converted to DNA sequences and these sequences are converted to the spliced form of data and protein form of data by cutting the introns according to the specified pattern and it is translated to mRNA form of data and mRNA is converted into protein form of data. The protein form of data is sent through the secure channel. The method does not really use DNA sequences, but only the mechanisms of the DNA function; therefore, the method is a kind of pseudo DNA cryptography methods. The method only simulates the transcription, splicing, and translation process of the central dogma; thus, it is a pseudo DNA cryptography method. Borda and Tornea proposed a secret writing method using DNA with the concept of one time pad [3]. Using XOR OTP tiles and chromosome indexing the message is encrypted. The technologies used by the different methodologies discussed in this paper are tabulated in Table 1.

TABLE I. TECHNOLOGY USED BY DIFFERENT ALGORITHMS

DNA Cryptography Algorithm	**Technology**
DNA Based Cryptography [2]	DNA substitution and one-time pads
DNA secret writing Techniques [3]	One-Time-Pad (OTP), DNA XOR OTP and DNA chromosomes indexing
An Encryption Scheme Using DNA Technology [5]	DNA digital coding PCR primers – A message is converted to DNA template in which primers are used as key to encode and decode the message
Cryptography with DNA binary strands [7]	DNA binary strands - Molecular checksum, PCR, gel Electrophoresis
A Pseudo DNA cryptography Method [9]	Transcription, Splicing, Translation-mRNA form of data into protein according to genetic code table and key send to the receiver in a secure channel

An Image Encryption Algorithm based on DNA Sequence Addition Operation [10]	DNA Sequence Matrix, DNA sequence addition using Logistic maps and complementarily.
YAEADNA Encryption Algorithm [12]	DNA Sequence Matching - data converted into pointers according to DNA strand taken and key send to the receiver in a secure channel
An Encryption Algorithm Inspired From DNA [13]	Symmetric key block cipher algorithm Transcription (DNA-RNA) – Translation (RNA- Protein) – message converted into matrix with initial permutation and XOR operation is performed with the key which is subjected to DNA module transcription and translation.
Hiding messages in DNA micro dots [14]	Base triplet Substitution and DNA Binary Strands

Guangzhao Cui et. al. encryption scheme is designed by using the technologies of DNA synthesis, PCR amplification, DNA digital coding and the theory of traditional cryptography [5]. Biological difficult issues and cryptography computing difficulties provide a double security safeguards for the scheme. Souhila Sadeg et. al. proposed a symmetric key block cipher algorithm which includes a step that simulates ideas from the processes of transcription (transfer from DNA to mRNA) and translation (from mRNA into amino acids) [13]. This algorithm is believed to be efficient in computation and very secure, since it was designed following recommendations of experts in cryptography and focuses on the application of the fundamental principles of Shannon: Confusion and Diffusion. A novel public-key system using DNA has been developed by Kazuo et. al. based on the one-way function [6]. The message-encoded DNA hidden in dummies can be restored by PCR amplification, followed by sequencing.

Taylor et. al have used a substitution cipher for plaintext encoding where base triplet is assigned to each letter of the alphabet, numeral and special characters and demonstrated a steganographic approach by hiding secret messages encoded as DNA strands among multitude of random DNA [14]. Qinghai has proposed new method to protect information, including representing information using biological alphabets to enhance the security of traditional encryption, using DNA primer for secure communication and key distribution, and using the chemical information of DNA bases for steganography [11]. Alice and Bob share a secret DNA sequence codebook. Alice can design a sequence that can maximally match one of the sequences in the codebook and then send the designed sequence to Bob through a public channel. When Bob receives the sequence he would use the non-matching letters in the private sequence as the encryption key. Knowing the public string only, an attacker cannot decrypt the transmitted information.

IV. IMPLEMENTATION ISSUE

Due to the limited progress in the field of DNA computing, the full potential of DNA Cryptography has not been completely tapped. The processes that take place at the molecular level have not been realized to its entirety outside an ultra-modern laboratory.

V. CONCLUSION

DNA binary strands support feasibility and applicability of DNA-based Cryptography. The security and the performance of the DNA based cryptographic algorithms are satisfactory for multi-level security applications of today's network. Certain DNA algorithms can resist exhaustive attack, statistical attack and differential attack. The field of DNA computing is still in its infancy and the applications for this technology have not yet been fully understood. DNA computing is viable and DNA authentication methods have shown great promise in the marketplace of today and it is hoped that its applications will continue to expand. DNA Cipher is the beneficial supplement to the existing mathematical cipher. If the molecular word can be controlled at will, it may be possible to achieve vastly better performance for information storage and security.

REFERENCES

[1] Adleman L M, "Molecular Computation of Solutions to Combinatorial Problems, Science",266:1021-1024, November 1994.

[2] Ashish Gehani, LaBean, T.H., and John H. Reif, "DNA-based Cryptography", Proceedings of DIMACS Workshop V on DNA Based Computers, American Mathematical Society, 1999. vol. 54. , pp 233–249.

[3] Borda M.E, Tornea O, "DNA secret writing Techniques" IEEE conferences 2010

[4] David Kahn, "The Codebreakers", McMillan, NY, 1967

[5] Guangzhao Cui, Limin Qin, Yanfeng Wang, Xuncai Zhang, "An Encryption Scheme using DNA Technology", IEEE Computer Engg. and Applications, (2008), pp 37-42.

[6] Kazuo Tanaka, Akimitsu Okamoto, Isao Saito, "Public-key system using DNA as a one - way function for key distribution", Biosystems, Vol. 81, Issue 1,(2005), pp 25–29.

[7] Leier A, Richter C, Banzhaf W, Rauhe H, "Cryptography with DNA binary strands", BioSystems 57(2000), pp 13-22

[8] Lipton R.J., "Using DNA to solve NP-complete problems", Science, (1995), 268(4), pp. 542-545.

[9] Ning Kang, "A pseudo DNA cryptography Method", http://arxiv.org/abs/0903.2693 ,2009

[10] Qiang Zhang, Ling Guo, Xianglian Xue, Xieopeng Wei, "An Image Encryption Algorithm based on DNA Sequence Addition Operation", IEEE 2009.

[11] Qinghai G, "Biological Alphabets and DNA based Cryptography", http:// www.asee.org/documents /sections /middle-atlantic/ spring-2010/ Biological-Alphabets-and-DNA-based-cryptography.pdf

[12] Sherif T. Amin, Magdy Saeb, Salah El-Gindi, "A DNA- based Implementation of YAEA Encryption Algorithm", IASTED International Conference on Computational Intelligence, 2006.

[13] Souhila Sadeg, Mohamed Gougache, N. Mansouri, H. Drias, "An Encryption algorithm inspired from DNA", IEEE (Nov 2010) pp 344 – 349.

[14] Taylor. C., Risca.V., and Bancroft.C, "Hiding messages in DNA Microdots", Nature (1999) :399, pp 533-534.

[15] Watson,J.D., Crick,F.H.C., "A Structure for De-oxy Ribose Nucleic Acid", Nature, vol. 25(1953), pp. 737-738

[16] Zhihua Chen, Xiutang Geng, Jin Xu, "Efficient DNA sticker algorithms for DES", IEEE 3rd International Conference on Bio-Inspired Computing, BICTA08, pp 15-22.